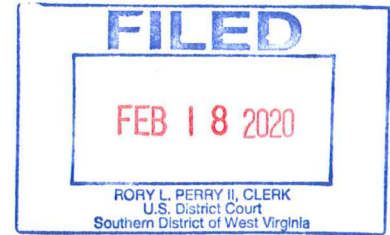


UNITED STATES DISTRICT COURT

for the
Southern District of West Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

iPhone, Model X, assigned to number 304-382-1266,
bearing the serial number DNQVP3J9JCLF, obtained
from NEDELCHO VLADIMIROV

Case No. 2:20-mj-00019

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment "A"

located in the Southern District of West Virginia, there is now concealed (identify the person or describe the property to be seized):
See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC 1341, 1343, 1349,
1956, 1957, 2314

Offense Description
Mail/wire fraud, money laundering, transfer of stolen goods, and conspiracy to violate those statutes

The application is based on these facts:

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Terry Hedrick, Special Agent USSS

Printed name and title

Sworn to before me and signed in my presence.

Date:

Judge's signature

City and state: Charleston, West Virginia

Dwane L. Tinsley, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

STATE OF WEST VIRGINIA
COUNTY OF KANAWHA, to-wit:

I, Terry Hedrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device described in Attachment A and the extraction from that property of electronically stored information described in Attachment B.

2. I am a duly sworn Special Agent of the United States Secret Service (USSS), having been so employed since October 2004 and having been in law enforcement since January 1989. My investigative duties focus primarily on conducting criminal investigations involving counterfeiting of United States currency, forgery, bank fraud, false loan applications, wire fraud, credit card fraud, false identification, other financial crime investigations, and protective intelligence/threat investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The warrant is requested to search the listed devices for evidence that relates to violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (Wire Fraud), 1349 (conspiracy), and 1956-1957 (Money Laundering).

4. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I know that the Device has capabilities that allows it to search and store information. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence related to the offenses being investigated and evidence that reveals or suggests who possessed or used the device.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a personal iPhone smartphone device (hereinafter, the "Device") which was in the possession of NEDELTCO VLADIMIROV (hereinafter "VLADIMIROV"), during his arrest at 5429 Hillbrook Drive, Cross Lanes, WV 25313, on February 10, 2020.

6. The Device, more particularly described in Attachment A, is currently in the possession of the U.S. Secret Service,

300 Summers Street, Charleston, WV 25301. I seek this warrant out to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data, more particularly described in Attachment B.

PROBABLE CAUSE

8. Since approximately December 2018, the United States Secret Service, the West Virginia State Police, Bureau of Criminal Investigation, the Putnam County Sheriff's Office, and the South Charleston Police Department (SCPD), together with Organized Retail Crimes (ORC) investigators from Kroger, CVS Pharmacy (CVS), and Target Corporation (Target), have been investigating VLADIMIROV for violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy), 1956-1957 (money laundering), and 2314 (transfer of stolen goods). These violations arise from VLADIMIROV's operation of a fraudulent scheme involving the interstate shipment of stolen goods.

9. As part of the scheme, VLADIMIROV has enlisted a crew of "boosters" who steal the merchandise from local retail stores and sell the stolen merchandise to VLADIMIROV, who then sells the stolen merchandise on online marketplaces such as eBay at a much higher price. Boosters usually have very specific items in mind

when perpetrating their schemes; usually driven at the direction of a fencing operation orchestrated by VLADIMIROV. Heavily targeted items tend to be those that are in high demand and of a high value relative to their size, ease of theft and profitability on the secondary market. Many of the known boosters are drug users addicted to controlled substances, who use the money received from VLADMIROV to support their drug habits.

BACKGROUND: ORIGIN OF INVESTIGATION

10. In November 2018, a CVS store in Hurricane, West Virginia, was impacted by a booster targeting Prevagen memory pills, which is an item commonly stolen and re-sold in fencing operations. Based on this information, a notice advising law enforcement and retail partners in the local area to "be on the lookout" (BOLO) for the subject was issued. Target Market Investigator Nicholas Niehaus (MI Niehaus) later contacted CVS Pharmacy ORC Manager Jose Varela and stated the same subject booster from the BOLO had also impacted Target stores in the Southern District of West Virginia area for several months.

11. From on or about September 10, 2018 to on or about December 29, 2018, known boosters Jonathan Marcus (hereinafter "Marcus") and Steven Anderson (hereinafter "Anderson") impacted South Charleston and Barboursville Target stores on multiple occasions for an estimated loss to Target of \$1,500. Target

Asset Protection ultimately identified the booster through an apprehension of Steven Anderson. Anderson was known to travel with Jonathan Marcus, who had also been identified through an apprehension.

12. During the booster interview, Marcus indicated to MI Niehaus that the two men would take the stolen merchandise to a local fencer known only as "Ned," who was later identified as NEDELTCCHO VLADIMIROV. Based on information developed in the interview with Marcus and by investigators subsequent to the interview, it is believed that VLADIMIROV has 15-20 drug users "boosting" for him. VLADIMIROV communicates with boosters by phone or electronic messaging service to provide lists of targeted items to the boosters. Following a theft, VLADIMIROV typically meets the booster at the Speedway convenience store and gas station located at 5296 Big Tyler Road, Charleston, West Virginia, which is 1.5 miles from the VLADIMIROV's residence. VLADIMIROV pays boosters anywhere from 10%-40% of the retail value of the stolen item.

13. In January 2019, MI Niehaus and ORC Manager Varela met with detectives with the SCPD. MI Niehaus and ORC Manager Varela provided detectives with the SCPD with the factual background of their investigation to that point, and the SCPD began their own investigation into prior retail theft arrests in their jurisdiction. The SCPD determined that numerous arrest

interviews were consistent and implicated VLADIMIROV as the suspected fencing operator in the South Charleston area.

BACKGROUND: BOOSTER APPREHENSIONS

14. On December 29, 2018, Marcus was apprehended at the South Charleston Target store for theft of two Nest Cameras valued at \$338.00. During the post-apprehension interview, Marcus indicated he was stealing the items to sell to VLADIMIROV, who buys stolen product from multiple subjects to resell online.

15. On September 11, 2019, Stephanie Miller (hereinafter "Miller") was apprehended at South Charleston, West Virginia, Target store for theft of a purse. During the interview, Miller indicated she steals items from area retail stores to sell to VLADIMIROV. Miller stated multiple subjects, herself included are sent lists from VLADIMIROV. Miller steals and sells the items to VLADIMIROV to support their drug habits.

BACKGROUND: SURVEILLANCE

16. Based on information received from retail investigators conducting interviews on theft subjects from Target located at 30 RHL Blvd South Charleston, West Virginia, investigators conducted surveillance of VLADIMIROV on three separate occasions: February 19-21, 2019, May 21-24, 2019, and October 22-24, 2019. Investigators observed VLADIMIROV shipping multiple packages a day at the post office located at the

intersection of Doc Bailey and Big Tyler Rd in Cross Lanes, West Virginia, as well as the FedEx location in Cross Lanes, West Virginia.

17. VLADIMIROV was observed on three occasions by Target, CVS, and SCPD investigators meeting subjects to purchase items in his Black BMW bearing West Virginia License Plate NNJ878. On almost every occasion, VLADIMIROV would travel to the U.S. Post Office located at 5306 Big Tyler Road, Charleston, West Virginia, in the early to mid-afternoon time. VLADIMIROV was seen meeting with known boosters and conducting transactions in public parking lots in Cross Lanes and Teas Valley, West Virginia. Detectives and Retail investigators have observed VLADIMIROV conduct multiple meetings with subjects known for theft activity in the Charleston, West Virginia area. VLADIMIROV conducts these transactions from inside his black 2004 BMW.

18. On October 23, 2019, surveillance was conducted of VLADIMIROV at the U.S. Post Office located at 5306 Big Tyler Road, Charleston, West Virginia. At 2:39 p.m., VLADIMIROV arrived at the post office in his black 2004 BMW bearing West Virginia license plate number NNJ878. VLADIMIROV entered the Post Office with several packages. At 2:41 p.m., VLADIMIROV exited the Post Office, returned to his vehicle, and left the property. Mobile surveillance was established at that time. At 2:57 p.m., VLADIMIROV arrived at the McDonald's restaurant

located at 4175 WV-34, Hurricane, West Virginia. At 2:59 p.m., VLADIMIROV remained in the black 2004 BMW, and a white female with a yellow sweatshirt and black backpack was observed on foot walking from behind the McDonald's approached and then entered the passenger side of the vehicle.

BACKGROUND: EBAY SALES

19. After validating information received from theft suspects and confidential informants provided by the SCPD and Putnam County Sheriff's Office, investigators contacted the eBay Investigations Unit in an attempt to identify the eBay account being used by VLADIMIROV. Investigators provided eBay with known identifiers of VLADIMIROV and were able to identify an active eBay account under his control: nedined. Based on these findings, investigators requested all transaction/sales data for the account from October 30, 2017 to October 29, 2019.

20. Review of the items being sold by VLADIMIROV on eBay include a multitude of categories: vitamins, over-the-counter medications, personal care items, electronics, pet-related items, tools, kitchen products, toys, RING doorbell systems, and home care items, among others.

21. From October 30, 2017 to October 29, 2019, approximately 3,676 items were sold on eBay by VLADIMIROV to buyers throughout both the United States and internationally.

VLADIMIROV'S sales on EBay totaled \$369,818.62 during this timeframe.

22. Most recently, an updated request for information was completed for eBay listing data from January 22, 2019 to January 22, 2020. In that time, VLADIMIROV listed and sold 1,761 items. During that time frame, VLADIMIROV's eBay sales totaled \$200,897.23.

23. Investigators have analyzed VLADIMIROV'S eBay account and were able to correlate reports of stolen items with items listed on VLADIMIROV's eBay account within days of theft offenses. Utilizing shortage inventory counts, items missing from Target, CVS, and Kroger stores were identified as being listed for sale or already sold on VLADIMIROV's account.

24. Investigators have continued to monitor known theft reports and can correlate theft incidents by subjects known to sell to VLADIMIROV with exact items being listed on VLADIMIROV's eBay account.

25. As of January 23, 2020, VLADIMIROV has had over 3,400 items listed for sale on his eBay account.

BACKGROUND: FINANCIAL INVESTIGATION

26. VLADIMIROV's bank accounts at City National Bank for the period December 2017 to November 2019 were analyzed, and the following information was derived:

(a) Account # XXX8889 - VLADIMIROV deposited numerous Postal money order, pay pal transfers, raise.com transfers (Raise.com is an e-commerce platform owned and operated by Raise that enables third-party sellers to sell new or used Gift Cards on a fixed-price online marketplace alongside Raise's regular offerings), and currency; VLADIMIROV withdraws a lot of money in currency out of this account, as evidenced by him taking out over \$76,000 from ATM withdrawals. Investigators believe this is some of the currency he used to pay for stolen goods from the boosters.

(b) A majority of the deposits into this account are from PayPal. PayPal is the avenue that processes payments when merchandise is bought and sold on EBay. These PayPal deposits totaled over \$263,000.00.

(c) VLADIMIROV transferred over \$250,000 from this City National Bank account to his savings account at City National Bank (Account# 9110074623).

(d) Total Deposits to VLADIMIROV'S Acct XXX8889 at City National Bank totaled over \$420,000.00.

(e) Over \$272,000 was transferred to VLADIMIROV's Savings account at City National Bank (\$155,000 was later transferred back to VLADIMIROV'S acct # 8889 at City National Bank, and he then wrote a check to transfer \$150,000 to his account at JP Morgan Chase Bank).

BACKGROUND: CONTROLLED SALES

27. On January 23, 2020, Confidential Informant 18-8400-009 (CI), also known as "John," made a controlled phone call to VLADIMIROV. The CI told VLADIMIROV that he had two Phillips Norelco electric razors from Target, and a meeting was set up at the Speedway parking lot at 5296 Big Tyler Rd, Charleston, West Virginia. Task Force Officer (TFO) K.A. Davis with the Violent Crime and Drug Task Force West drove the CI to the meeting location. VLADIMIROV arrived on scene in his black 2004 BMW, and

the CI got into the passenger side of the vehicle with him. VLADIMIROV looked at the items and paid the CI \$40. The CI then exited the vehicle, reentered the undercover vehicle with TFO Davis. The CI delivered the U.S. currency to TFO Davis and was debriefed.

28. On January 28, 2020, TFO Davis, acting in an undercover capacity, made a controlled phone call to VLADIMIROV. TFO Davis claimed to be friends with "John" and told VLADIMIROV that he had a RING doorbell. VLADIMIROV agreed to meet TFO Davis at the Speedway parking lot at 5296 Big Tyler Rd, Charleston, West Virginia. VLADIMIROV arrived on scene in his black 2004 BMW, and TFO Davis entered the vehicle with him. TFO Davis produced the stolen Ring door bell system and stated, "I don't know how much I get can get for this." VLADIMIROV then used his mobile electronic device to look up the item on eBay and told TFO Davis he could pay him \$35. TFO Davis agreed. TFO Davis then told VLADIMIROV that he wanted to make more money and asked what items VLADIMIROV wanted. VLADIMIROV stated that the more expensive the item the more TFO Davis would get paid. VLADIMIROV indicated that he was looking for Apple products like iPad Pro's.

29. On January 29, 2020, TFO Davis, acting in an undercover capacity, made a controlled phone call to VLADIMIROV. TFO Davis told VLADIMIROV that he had some more items to sell.

VLADIMIROV agreed to meet TFO Davis at the Speedway parking lot at 5296 Big Tyler Rd, Charleston, West Virginia. VLADIMIROV arrived on scene in his black 2004 BMW, and TFO Davis entered the vehicle with him. TFO Davis produced the stolen tooth brushes and stated "I got these from CVS and the tag on the shelf said they were \$150.00." VLADIMIROV then became very suspicious and asked to see TFO Davis's phone. VLADIMIROV asked what kind of phone it was, and TFO Davis responded that he did not know because it was a phone his mom gave him and it is on her plan. VLADIMIROV then asked to see the phone. TFO Davis handed VLADIMIROV the phone. VLADIMIROV then inspected it by examining the call history and text messages as well as cycling through the applications. VLADIMIROV then closed all of the applications running on the phone, which cancelled the covert recording application that was recording the controlled sale. VLADIMIROV then told TFO Davis that he did not know if he wanted the electric toothbrushes because he sells all the merchandise on eBay, and other eBay listings had the item listed at \$35.00. After some deliberation, VLADIMIROV decided that he could give TFO Davis \$30 for the electric tooth brushes. TFO Davis then stated that he would call VLADIMIROV again tomorrow, and VLADIMIROV agreed that would be fine. No audio or video of this controlled sale was obtained due to technical difficulties.

TECHNICAL TERMS

30. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate

the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term-IP addresses, while other computers have dynamic—that is, frequently changed-IP addresses.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such devices. This information can sometimes be recovered with forensics tools.

32. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can

be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the

purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

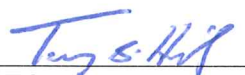
34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e) (2) (B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION


36. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Further your affiant sayeth naught.



SPECIAL AGENT TERRY HEDRICK,
UNITED STATES SECRET SERVICE

Sworn to before me, and subscribed in my presence, this 18th
Day of February, 2020.



THE HONORABLE DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. The property to be searched is as follows: an iPhone Model X smartphone, assigned to number 304-382-1266, bearing the serial number DNQVP3J9JCLF, encased in red otter box protective covering, and currently located in the possession of the U.S. Secret Service, 300 Summers Street, Charleston, WV 25301.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (Wire Fraud), 1349 (conspiracy), and 1956-1957 (Money Laundering), since on or about October 30, 2017, including:

- a. Lists of co-conspirators and related identifying information;
- b. Transactions and prices concerning stolen items, as well as dates, places, and amounts of specific transactions;
- c. Any information related to sources of stolen items (including names, addresses, phone numbers, or any other identifying information), including but not limited to known sources Brian Kearsey, Johnathan Chapman, Kayla Burgess, Jonathan Marcus, Steven Anderson, Mike Doss, Shawn Patrick, Kayla Powell, Cassidy Wentz, Brittany Sierra, Sarah Payne, Stephanie Miller, and Danielle Utt;
- d. Any information recording VLADIMIROV's schedule or travel from October 30, 2017 to the present;
- e. All bank records, checks, credit card bills, account information, and other financial records;
- f. All eBay and Paypal records;
- g. Any record of a business locations or other addressed which would identify recent travel history of all the above including internet search, any map program, and/or GPS information found on the Device.
- h. Any email, text message, or voice mail message via text, found on the Device which would identify persons to whom VLADIMIROV exchanged United States currency during a business or personal monetary transaction of any kind.

i. Any photographs or identifying information of potential co-conspirators.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.